



# WSO2 IDENTITY SERVER

---

Prabath Siriwardena

[prabath@wso2.com](mailto:prabath@wso2.com) | [prabath@apache.org](mailto:prabath@apache.org)

# WSO2 IDENTITY SERVER

## Overview

---

- Addresses critical IAM needs both in customer IAM and workforce IAM spaces
- Most of the WSO2 IS deployments are to address CIAM needs
- The key focus area is **Federated Identity Management and Web Single Sign On (SSO)**
- Extensive support for open standards - no vendor locking
- Large scale deployments over millions of users
- Rich ecosystem with 40+ connectors (<https://store.wso2.com/store/assets/isconnector/list>)
- Support for multi-tenancy
- Web based management console and user portal (with easily customizable theme)
- Extensible product architecture to address complex IAM needs
- Docker friendly deployment
- Latest release (July 2018) - WSO2 Identity Server 5.6.0

# WSO2 IDENTITY SERVER

## Focus Areas

---

- **Web single sign-on and identity federation**
- **Identity broker**
- **Strong/Adaptive Authentication**
- Accounts management and identity provisioning
- Fine-grained access control
- API security
- Identity analytics

# SINGLE SIGN-ON & IDENTITY FEDERATION

---

- 90% of the WSO2 Identity Server deployments are used to enable SSO and Identity Federation.
- Support for multiple heterogeneous SSO standards (SAML, OIDC, WS-Federation, CAS) enables WSO2 Identity Server to build a unified SSO platform across multiple on-prem and cloud service providers.
- Out of the box integration with SaaS vendors - Salesforce, Google Apps, AWS, etc.
- Out of the box integration with Facebook, Google, Yahoo!, Windows Live, Twitter, LinkedIn, etc

# SINGLE SIGN-ON & IDENTITY FEDERATION

## Open Standards

---

- SAML 2.0
- OpenID Connect (OAuth 2.0)
- WS-Federation
- CAS ( Developed and contributed to the product by a customer)
- OpenID
- GSMA Mobile Connect
  - WSO2 Telco, powered by WSO2 Identity Server, together with the MNOs, which include Aircel, Bharti Airtel, Idea, Tata Teleservices Ltd, Telenor and Vodafone, serve more than 800 million consumers across India



# SINGLE SIGN-ON & IDENTITY FEDERATION

## Policy-Based Access

---

- Based on
  - Authenticated user's roles
  - Authenticated user's attributes
  - Time
  - The identity store the authenticated user belongs to
- Ability to plugin custom data sources in the process of decision making

# SINGLE SIGN-ON & IDENTITY FEDERATION

## Social Login

---

- Enable Social Login by service provider
- Facebook, LinkedIn, Twitter, Google, Yahoo, Microsoft Live





# SINGLE SIGN-ON & IDENTITY FEDERATION

## Outbound Identity Federation

---

- WSO2 Identity Server can federate users to external identity providers.
- Supports outbound federation with SAML, OIDC, WS-Federation, OpenID
- The GSMA Mobile Connect, connector in WSO2 Identity Server lets you incorporate Mobile Connect into the current login flows (based on SAML, OIDC, etc) with zero code change
- BYOID (Bring Your Own IDentity) - ability to map enterprise accounts with federated logins





# SINGLE SIGN-ON & IDENTITY FEDERATION

## Just In Time Provisioning

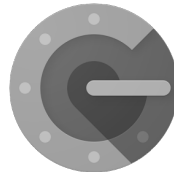
---

- Just in time provision users to a selected identity store, from different federated identity providers
- Ability to trigger outbound provisioning in the process of JIT provisioning
- WSO2 Identity Server prompts the user to enter any missing (but required) attributes during the JIT provisioning.

# STRONG AUTHENTICATION

---

- Strong authentication with FIDO U2F, OTP over SMS/Email, TOTP, Certificates, Duo Security, RSA SecurID, mePin
- Support for biometrics with Veridium



# ADAPTIVE AUTHENTICATION

---

- Script-based control over the authentication flow
- Step up authentication based on;
  - Environmental attributes (e.g: any HTTP header, geo-location)
  - User attributes / roles (e.g: admins always log with MFA)
  - User behavior (e.g.: number of failed login attempts, geo-velocity)
  - Risk

# IDENTITY BROKER

---

- Transform identity tokens to and from multiple heterogeneous identity federation and provisioning protocols (SAML, OIDC, WS-Federation, OpenID, SCIM, SPML)
- Mostly used with Identity Federation use cases.

# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

---

- Supports user onboarding, account verification, identity provisioning
- Self registration, password recovery/reset, update user profile, account mapping .
- Connects to multiple identity stores (LDAP, AD, Database)
- Multi-level approval workflows.

# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## Multiple Identity Stores

---

- Support for heterogeneous identity stores: database, LDAP, AD
- Largest deployment of WSO2 IS in Saudi Arabia (4M+ users in a MS SQL database)
- State of Arizona uses WSO2 IS for both CIAM and workforce IAM over a MSSQL database and AD

# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## Self Service


---

- Self registration
- Password recovery/reset
- Update user profile
- Account mapping
- Ability to plugin custom interceptors in all the self service flows helps customers to add their business logic for validation - for example check if user exists in Salesforce before adding the user into the system.


# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## Self Service

---

 User Portal


### My Profile



Update your profile or add multiple user profiles.

[View details](#)


### Account Recovery



Update account recovery challenge questions.

[View details](#)


### Change Password



Change current account password.

[View details](#)


### Associated Accounts



Manage Associated User Accounts & Federated IDs.

[View details](#)


### Authorized Apps



Manage your authorized applications.

[View details](#)

### My Login Sessions



Manage login sessions.

[View details](#)





# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING


## Approval Workflows


- Multi-layered
- Multiple approvers in a given layer - by role or name of the approver
- Trigger conditions, e.g. 'trigger workflow only if user is in the admin group'


**Manage**


 Workflow Engagements

 Add

 List

 Workflow Definitions

 Add

 List

[Home](#) > [Manage](#) > [Workflow Engagements](#) > [List](#)

[? Help](#)

### Workflow Association List

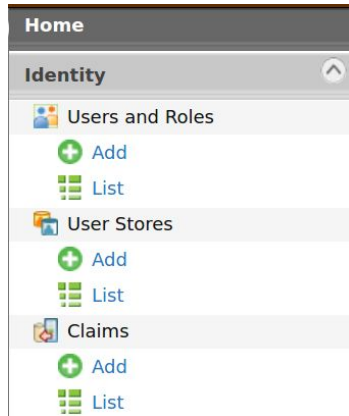
 [Add New Workflow Engagement](#)

Association Name	Operation	Workflow Name	Actions
add_user	Add User	add_user	 Enable  Delete

# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## User Administration

- Perform CRUD operations on users/roles
- User/role assignments
- Terminate user sessions
- Force user password reset



Home > Identity > Users and Roles > List > Users

### Users

Search Users	
Select Domain	PRIMARY
Enter user name pattern (* for all)	* Search Users
Select Claim Uri	Select
Count Users	
Select Domain	foo
Enter search pattern (applied on user name by default)	% Count Users
Select Claim Uri	Select
foo	3

Name	Actions
admin	<a href="#">Change Password</a> <a href="#">Assign Roles</a> <a href="#">View Roles</a> <a href="#">Delete</a> <a href="#">User Profile</a>
dhanik	<a href="#">Change Password</a> <a href="#">Assign Roles</a> <a href="#">View Roles</a> <a href="#">Delete</a> <a href="#">User Profile</a>
peter	<a href="#">Change Password</a> <a href="#">Assign Roles</a> <a href="#">View Roles</a> <a href="#">Delete</a> <a href="#">User Profile</a>
thilini	<a href="#">Change Password</a> <a href="#">Assign Roles</a> <a href="#">View Roles</a> <a href="#">Delete</a> <a href="#">User Profile</a>



# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## Inbound/Outbound Provisioning

---

- Inbound provisioning with SCIM/SOAP APIs
- Outbound provisioning with SCIM/SPML/Salesforce/Google Apps
- Controlled by policies



# ACCOUNTS MANAGEMENT & IDENTITY PROVISIONING

## Consent Management

---

- Manage user consent related to PII processed by the identity provider.
- Manage user consent related to PII processed by 3rd party applications.
- Consent management portal
- Kantara consent receipts

# FINE-GRAINED ACCESS CONTROL

---

- Supports fine-grained access control with XACML.
- WSO2 IS acts as the XACML PAP, PDP and connects with multiple PIPs.
- Exposes PDP as a RESTful API
- Used by AL ELM to control access to one of their portal built with Liferay.
- Verifone uses XACML to control access to their APIs

# FINE-GRAINED ACCESS CONTROL

## XACML 3.0

---

- Acts as a Policy Decision Point (PDP) and a Policy Administration Point (PAP)
- Multiple pluggable Policy Information Points (PIP)
- PDP is exposed as a RESTful API
  - Supports JSON/REST Profile for XACML 3.0
- Enforces policies in login and provisioning flows
- AL ELM is using XACML to perform fine-grained access control against users login to their Liferay portal

# FINE-GRAINED ACCESS CONTROL

## XACML 3.0

- Wizard for creating policies

Home > Entitlement > PAP > Policy Administration

### Policy Administration

[+ Add New Entitlement Policy](#)

Policy Type **ALL**

Search Policy \*



Select all in this page | Select none



Delete



Publish



Publish

#### Available Entitlement Policies

<input type="checkbox"/>	authn_role_based_policy_template	Policy	Edit	Versions	Publish To My PDP	Try	View Status
<input type="checkbox"/>	authn_scope_based_policy_template	Policy	Edit	Versions	Publish To My PDP	Try	View Status
<input type="checkbox"/>	authn_time_and_role_based_policy_template	Policy	Edit	Versions	Publish To My PDP	Try	View Status
<input type="checkbox"/>	authn_time_and_scope_based_policy_template	Policy	Edit	Versions	Publish To My PDP	Try	View Status
<input type="checkbox"/>	authn_time_and_user_claim_based_policy_template	Policy	Edit	Versions	Publish To My PDP	Try	View Status

Home > Entitlement > PAP > Policy Administration > Create XACML Policy

[? Help](#)

### Create XACML Policy

Entitlement Policy Name\*

Rule Combining Algorithm

First Applicable



Entitlement Policy Description

^ This Policy is going to be evaluated, Only when followings are matched....

IdentityUser



is



equal



END

^ Define Entitlement Rule(s)

^ Define Policy Obligations or Advices

Obligation Type

Id

Effect

Attribute Value

Obligation



Permit



Rule Id

Rule Effect

Action

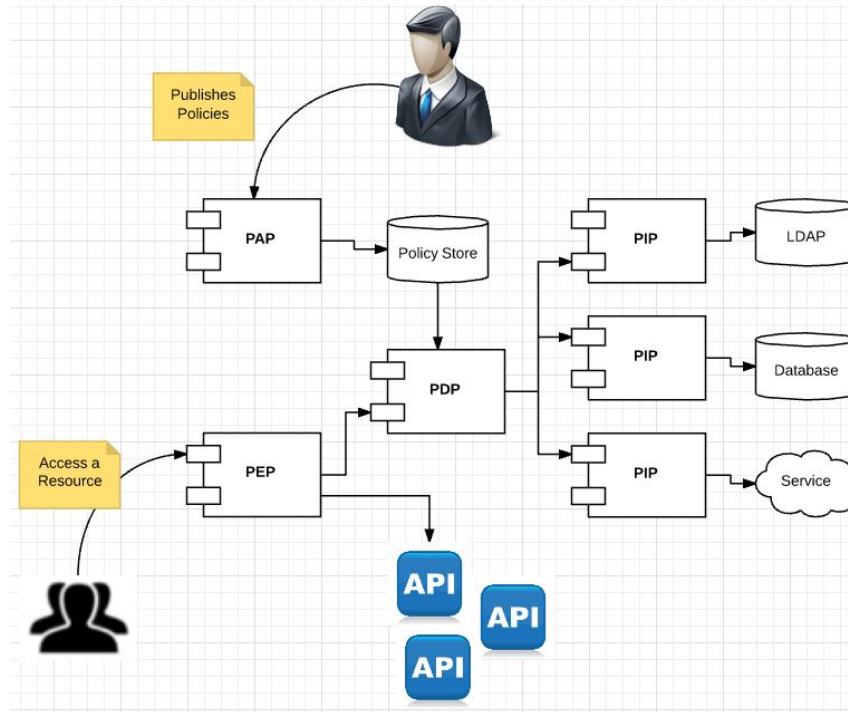
No rules defined yet

Finish

Cancel

# FINE-GRAINED ACCESS CONTROL

## XACML Architecture



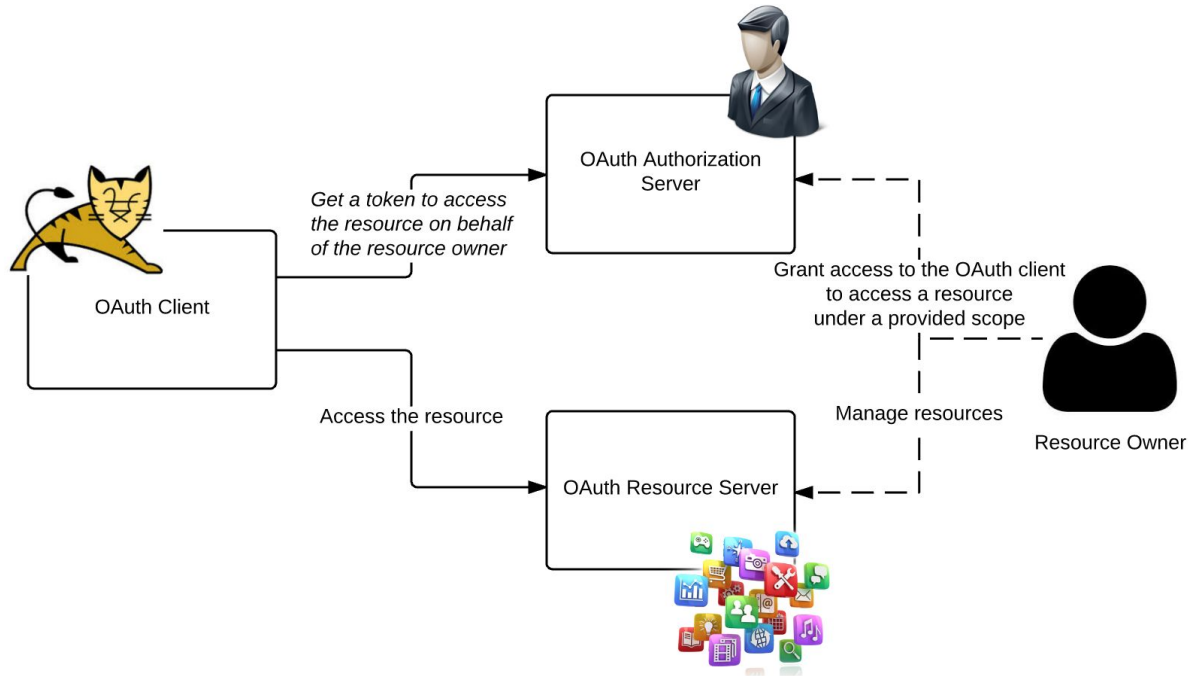


# API SECURITY

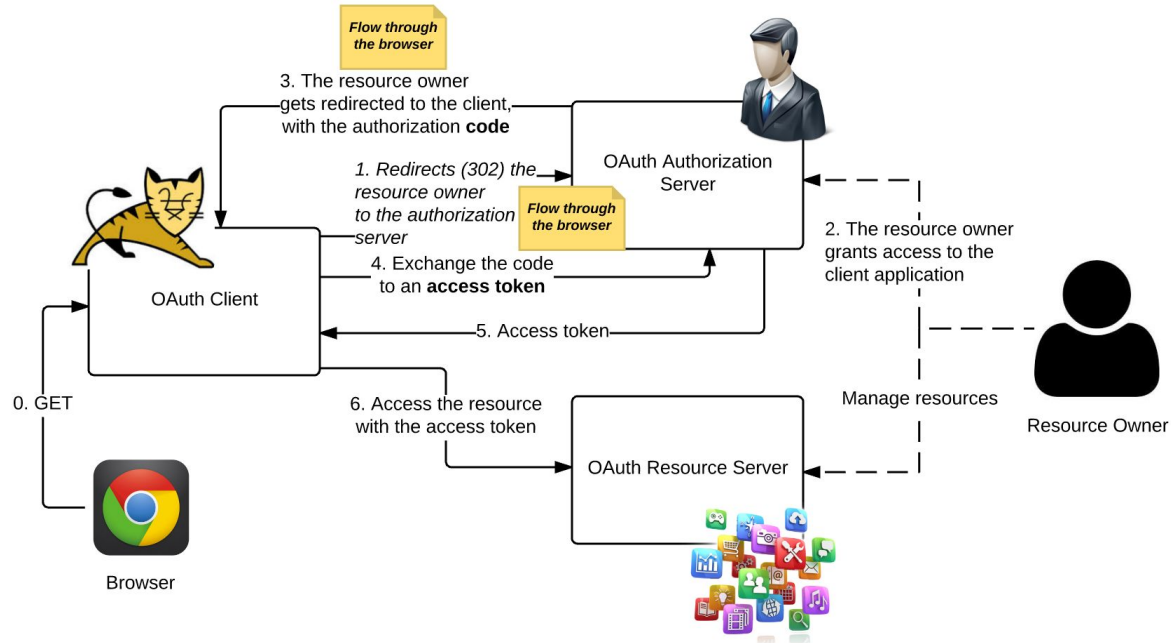
---

- Comprehensive support for OAuth 2.0 and related profiles.
- WSO2 Identity Server acts as a token issuer, verifier and an STS.
- Embedded in all WSO2 API Manager deployments over a 100+ customer base as the key manager (including StubHub, Fidelity)

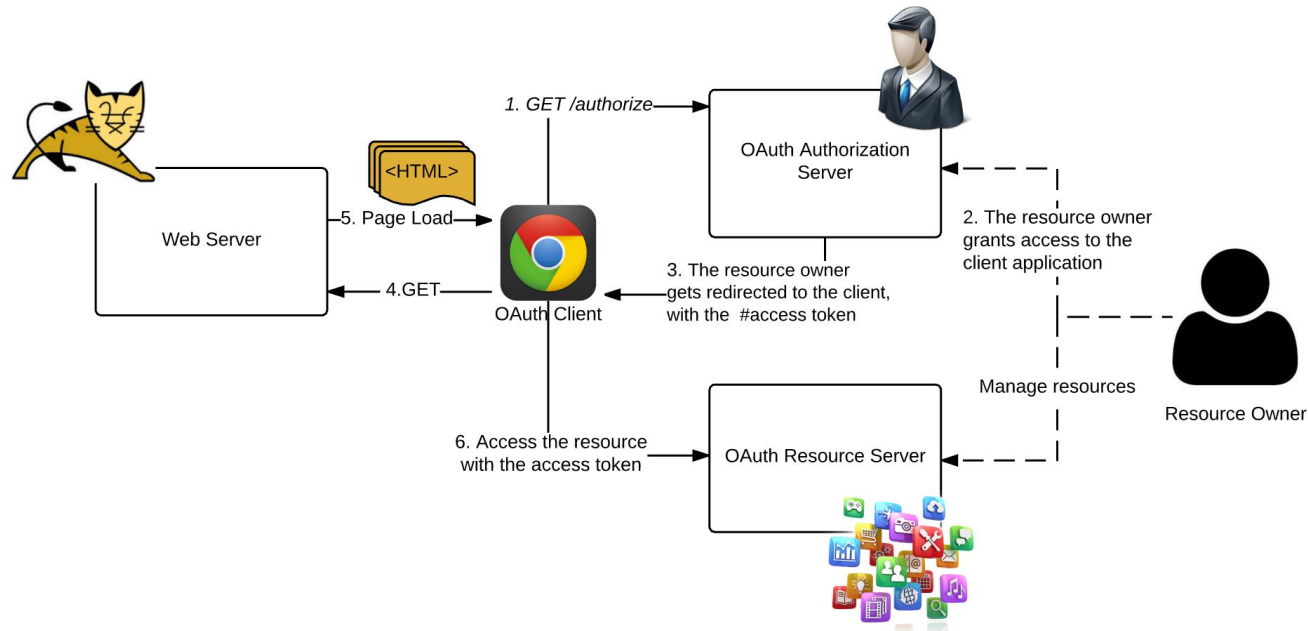
# OAuth 2.0



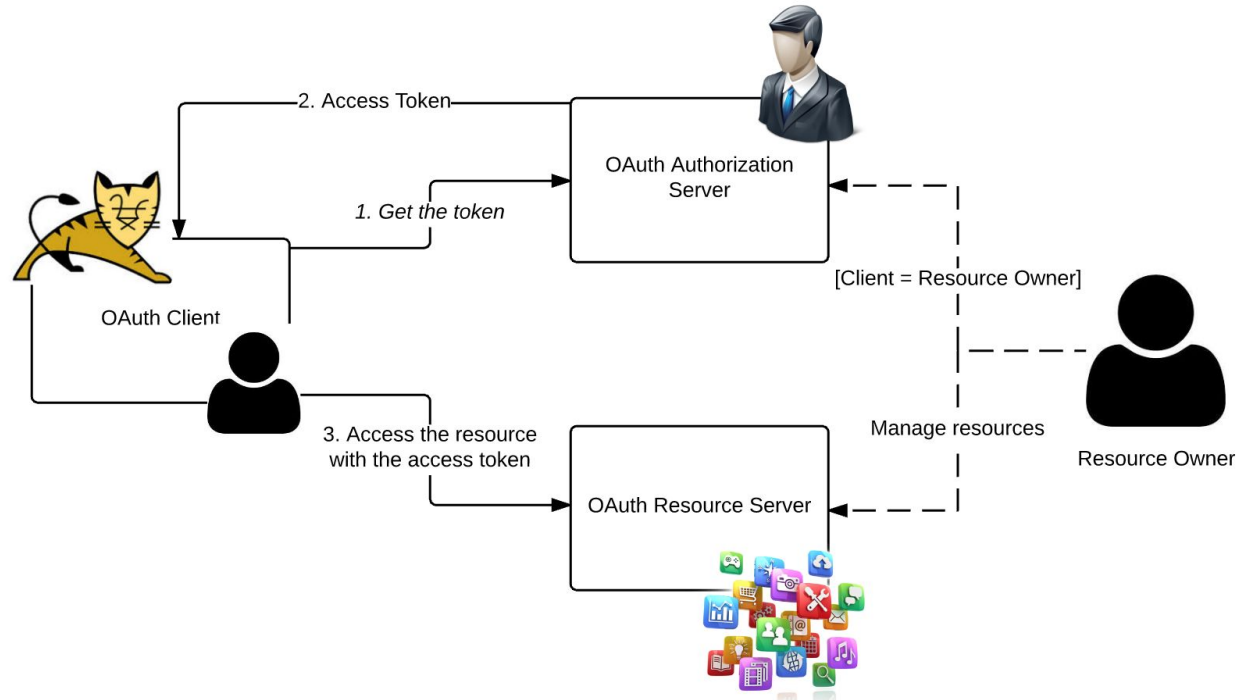
# AUTHORIZATION CODE



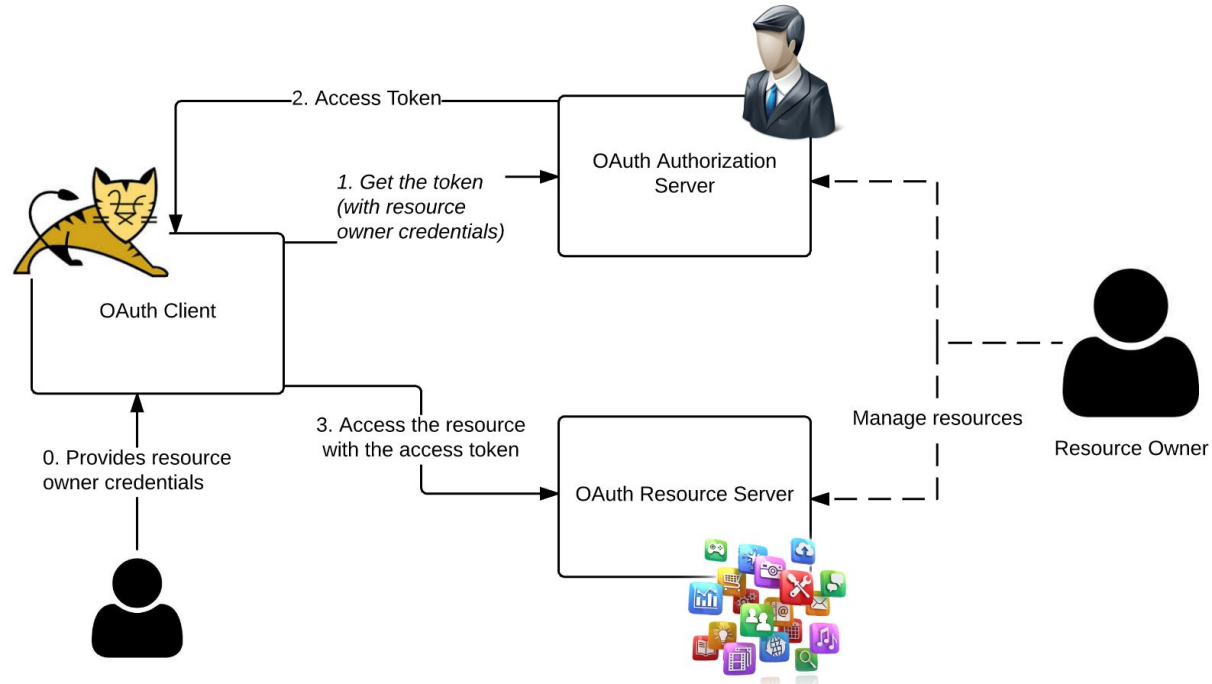
# IMPLICIT



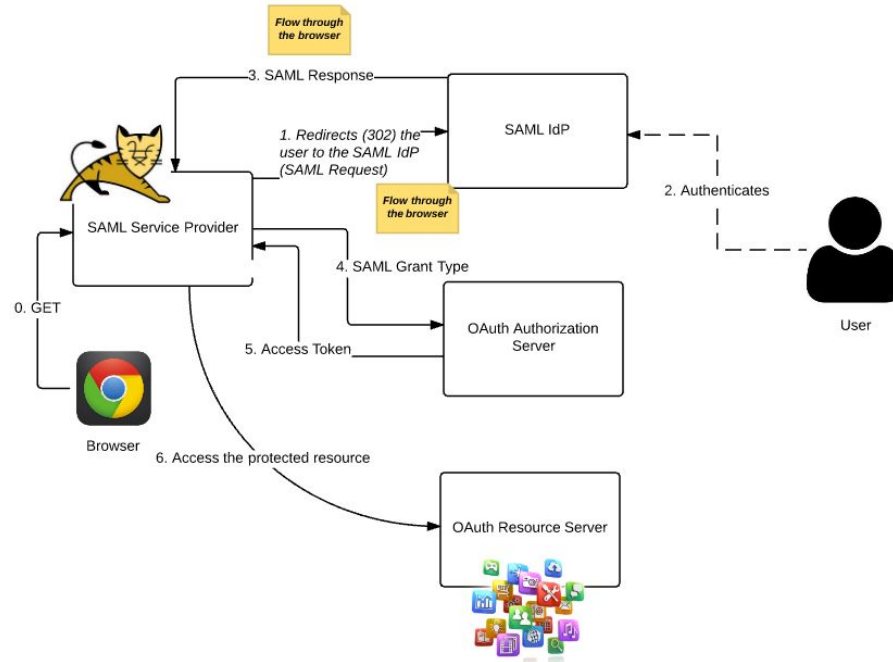
# CLIENT CREDENTIALS



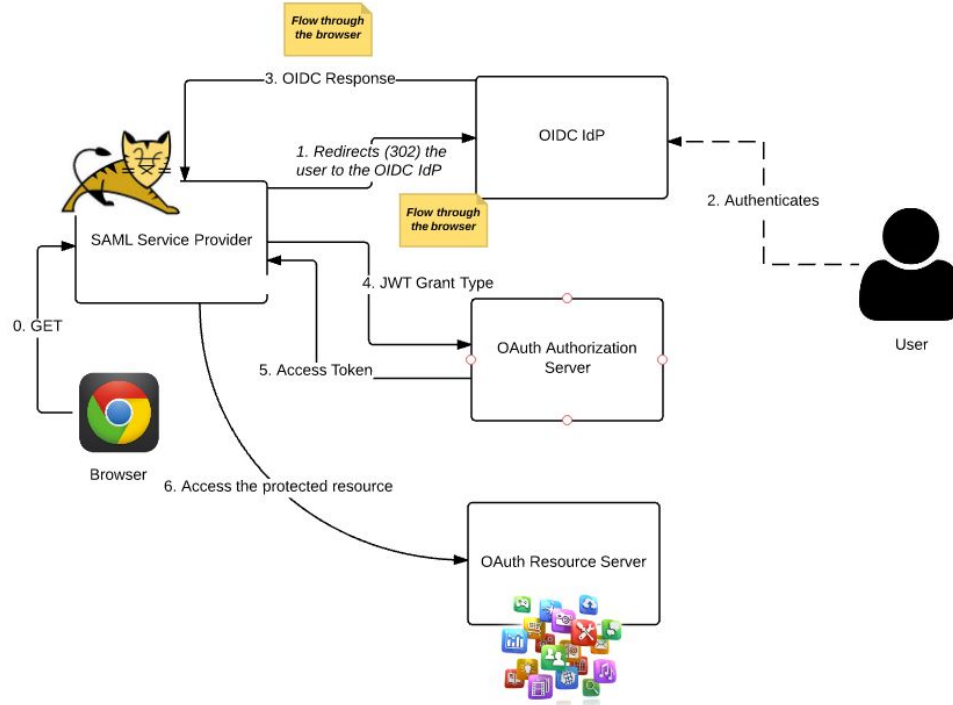
# RESOURCE OWNER PASSWORD



# FEDERATED API ACCESS

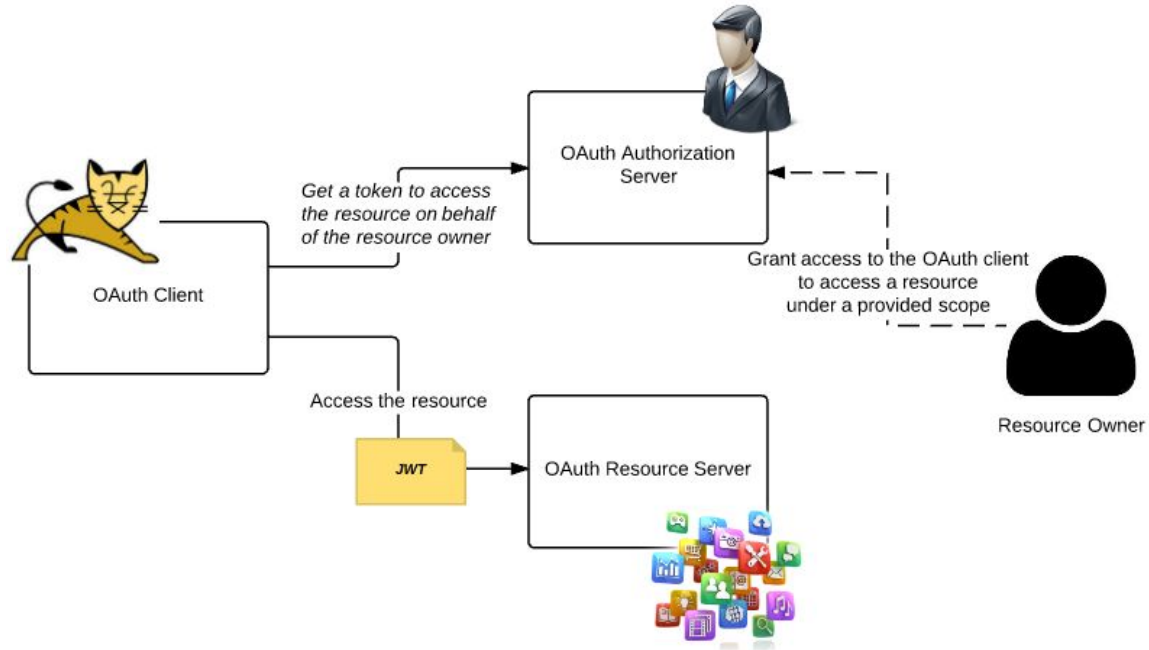


# FEDERATED API ACCESS

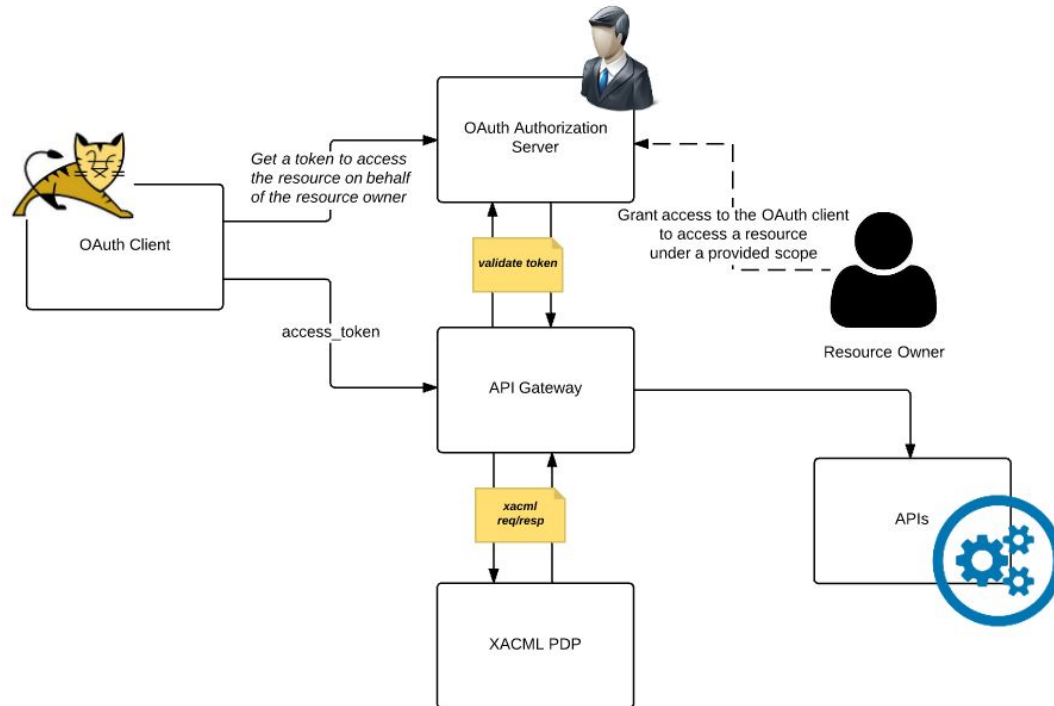




# SELF CONTAINED ACCESS TOKENS



# FINE-GRAINED ACCESS CONTROL FOR APIs



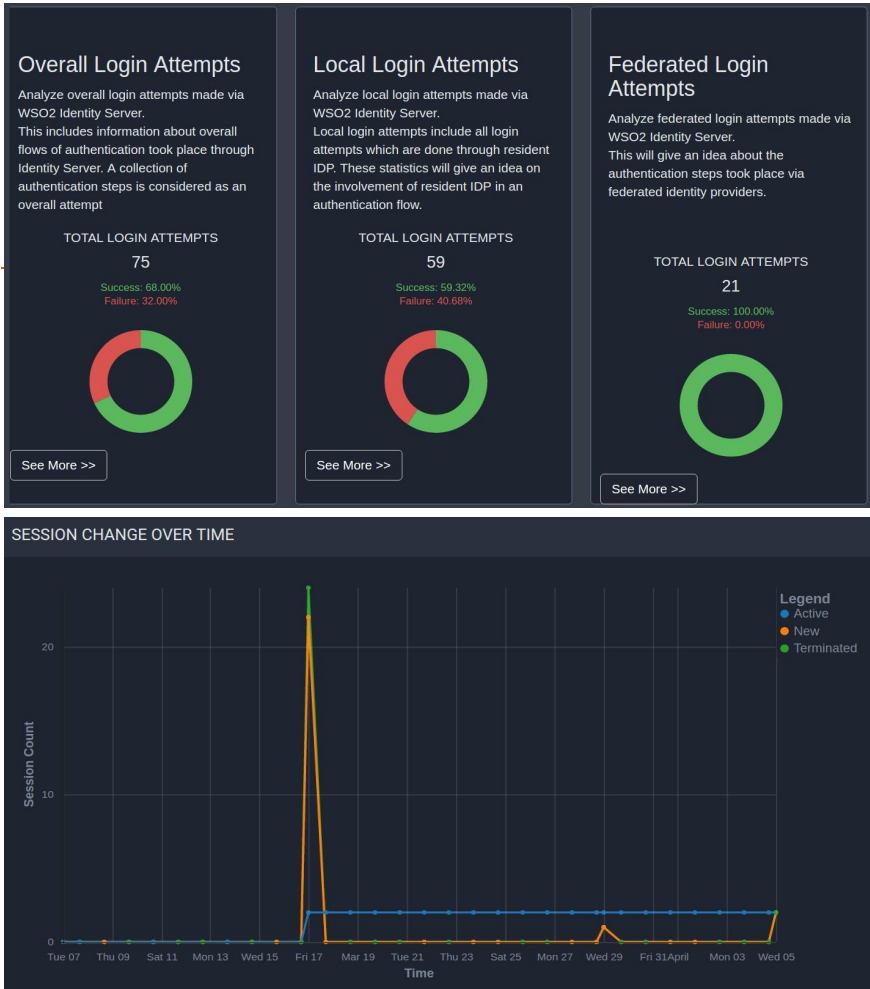
# API SECURITY

---

- Comprehensive support for OAuth 2.0
  - Authorization Code / Implicit / Password / Client credentials grant types.
  - SAML grant type for OAuth 2.0
  - JWT grant type for OAuth 2.0
  - Token Introspection
  - Dynamic Client Registration
  - Proof Key for Code Exchange (PKCE)
- Used as the key manager for all WSO2 API Manager deployments.
- Self-contained access tokens
- Based on customer requirements developed custom grant types for Kerberos and NTLM

# IDENTITY ANALYTICS

- Login analytics by success/failed login attempts - service provider and the federated identity provider.
- Session analytics - by users - the length of each session.
- Detect anomalous login behaviors.



# IDENTITY CONNECTOR STORE

<https://store.wso2.com/store/assets/isconnector/list>

The screenshot displays the WSO2 Identity Connector Store interface. On the left, a dark sidebar contains a 'Filter by' section with dropdowns for 'IS Versions' and 'Extension Type', and a 'Tags' section with buttons for 'Biometric', 'GSMA', 'HardwareToken', 'IS-5.2.0', 'IS-5.3.0', 'MobileConnect', 'Oauth-2.0', 'grant-type', 'Password-Reset', 'Enforcer', 'SocialLogin', 'Token', and 'Twofactor'. The main area features a search bar at the top with the text 'Search in IS Connectors', a 'My bookmarks' link, and a 'Sort by : Date/Time' dropdown. Below this, a grid of identity connectors is shown, each with a logo, name, version, and star rating. The connectors include:

- Pinterest Authenticator (Pinterest logo, V1.0.0, 5 stars)
- Mobile Connect Authenticator (Mobile Connect logo, GSMA V1.0.1, 5 stars)
- SAML Authenticator (SAML logo, WSO2 V5.1.6, 5 stars)
- FIDO Authenticator (FIDO logo, YUBICO V5.1.6, 5 stars)
- CAS Inbound Authenticator (CAS logo, CAS V1.0.2, 5 stars)
- X509 Certificate Authenticator (X509 logo, X509 V2.0.2, 5 stars)
- SCIM Provisioning Connector (SCIM logo, WSO2 V5.1.2, 5 stars)
- Salesforce Provisioning Connector (Salesforce logo, Salesforce V5.1.2, 5 stars)
- SPML Provisioning Connector (SPML logo, SPML V5.1.2, 5 stars)
- Google Provisioning Connector (Google logo, Google V5.1.2, 5 stars)
- Reddit Authenticator (Reddit logo, Reddit V1.0.1, 5 stars)
- Inwebo Provisioning Connector (Inwebo logo, Inwebo V1.0.0, 5 stars)
- RSA SECURED Authenticator (RSA SECURED logo, RSA V1.0.0, 5 stars)
- PassiveSTS Federator (PassiveSTS logo, WSO2 V5.1.2, 5 stars)

The footer of the interface shows 'WSO2 Store | © 2016 WSO2 Inc.'



OPEN TECHNOLOGY FOR YOUR AGILE DIGITAL BUSINESS

# THANK YOU

[wso2.com](https://wso2.com)

